09.19.05

AF IFW
2137

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Gerald R. Malan et al.

Serial No.: 09/855,808

Filed: May 15, 2001

Group Art Unit: 2137

Examiner: Courtney Fields

For: METHOD AND SYSTEM FOR DETECTING, TRACKING AND BLOCKING DENIAL OF SERVICE ATTACKS OVER A COMPUTER NETWORK

Attorney Docket No.: UOM 0234 PUS

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal Brief from the final rejection of claims 1-19, 21-23 and 26-33 of the Advisory Action mailed on July 14, 2005 for the above-identified patent application.

I. REAL PARTY IN INTEREST

The real party in interest is The Regents of the University of Michigan ("Assignee"), a non-profit corporation organized and existing under the laws of the state of Michigan, and having a place of business at 3003 S. State Street, Ann Arbor, MI 48109, as

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8

I hereby certify that this paper, including all enclosures referred to herein, is being deposited with the United States Postal Service as first-class mail, postage pre-paid, in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, U.S. Patent & Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 on:

9-16-05	David R. Syrowik	
Date of Deposit	**Name of Person Signing**	**Signature**

set forth in the assignment recorded in the U.S. Patent and Trademark Office on May 15, 2001 at Reel 011813/Frame 0402.

II. RELATED APPEALS AND INTERFERENCES

There is a related appeal in application Serial No. 09/855,810 for: "Method and System for Reconstructing a Path Taken By Undesirable Network Traffic," which may directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-19, 21-23 and 26-33 are pending in this application. Claims 1-19, 21-23 and 26-33 have been rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

An Amendment after final rejection was filed on June 17, 2005, and has been accepted for entry.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter is a method and a system for detecting, tracking and blocking one or more denial of service (*i.e.*, DoS) attacks over a computer network as indicated by the following: a) the title of the application; b) the first sentence of the abstract; c) the field of the invention; d) the first paragraph under the heading "Summary of the Invention"; and e) independent claim 1 and dependent claims 21 and 28.

The system of claim 1 includes a collector (20, 20b, 20c and 20d of Figures 4 and 7; also, "means for detecting" in claim 19) adapted to receive a plurality of data packet flow statistics from a routing system (22, 22b, 22c and 22d of Figures 4 and 7) of the computer network and to process the plurality of data packet flow statistics to detect one or more data packet flow anomalies and to generate a signal representing the one or more data packet flow anomalies. A controller (24, 24b of Figures 4 and 7; also, "means for tracking" in claim 19) is coupled to the collector to receive the signal. The controller is constructed and arranged to respond to the signal by tracking attributes related to the one or more data packet flow anomalies to at least one source. The controller may be constructed and arranged to block the one or more data packet flow anomalies (independent claim 1 but not independent claims 19 and 27).

As indicated at page 14, lines 5-12, and with reference to Figures 4 and 7 reproduced hereinbelow, data packet flow statistical information can include the number of packets which have been communicated between computer system 16, the duration of communication between each of the computer systems 16, the total number of packets communicated over each LAN, as well as other various data packet flow statistical information.

The collector 20 is adapted to receive the data packet flow statistical information from the routing system 22 and to process the data packet flow statistical information to detect data packet flow anomalies, as indicated at page 14, lines 20-22.

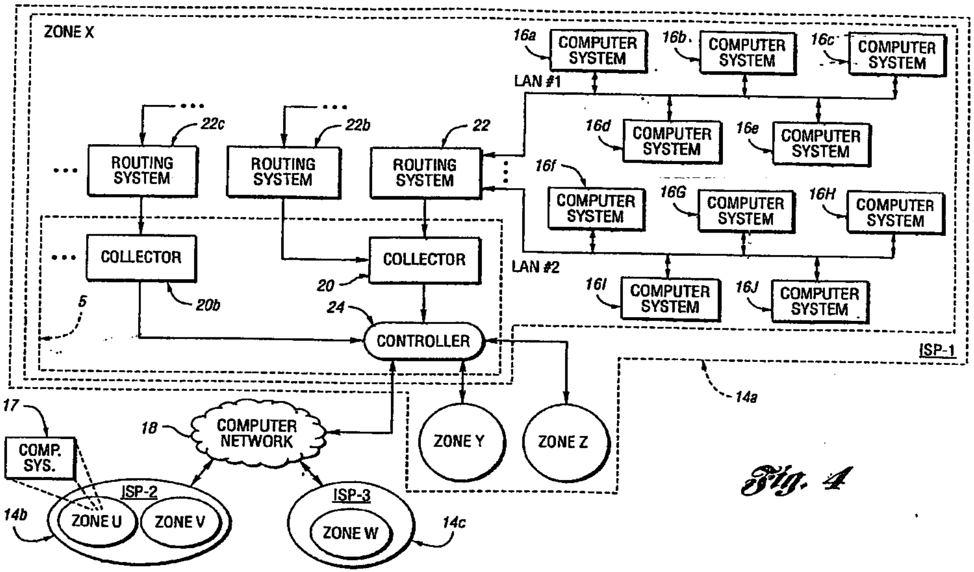


Fig. 4

As indicated at page 16, lines 10-13, flow-based statistics include a set of packets that are related to the same logical traffic flow. The concept of flow-based statistics is generally defined as a stream of packets that all have the same characteristics such as source address, destination address, protocol type, source port, and destination port.

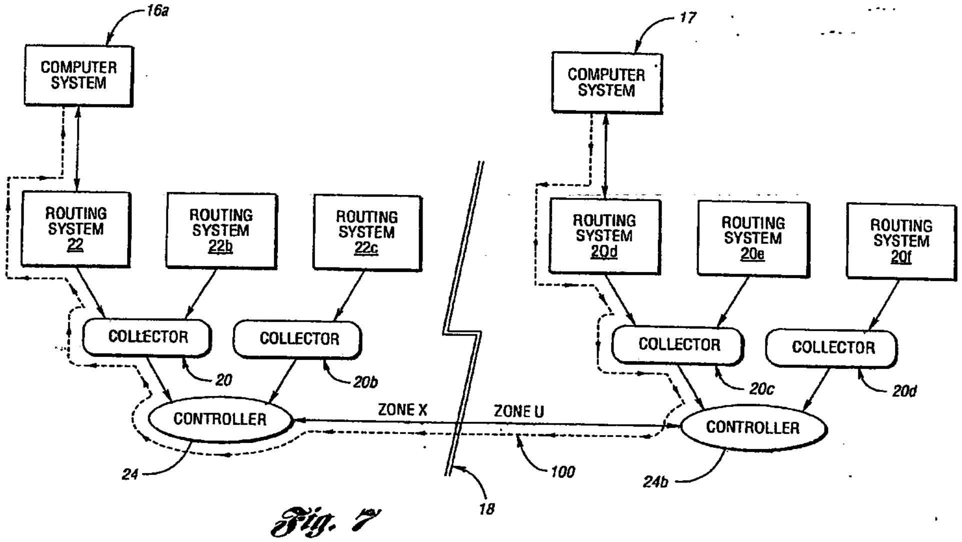


Fig. 7

As indicated at page 17, line 26 through page 18, line 14, the controller 24 can apply several approaches to track or trace the DoS attack back to its origin such as directed tracing or distributed correlation. In directed tracing, information related to the computer network system topology is processed to work backward toward the source or origin (*i.e.*, computer system 17) of the DoS attack. Directed tracing relies on the fact that both the router system's incoming interface statistic for a DoS attack and information related to the computer network system 10 topology are known to determine what routers are upstream of a particular link that carried the DoS attack packet. With this knowledge, upstream routers can then be queried for their participation in transiting the attack packet. Since these upstream routers are looking for a specific attack signature, it is much easier to find the statistics related to the attack packet.

In distributed correlation, the controller 24 compares the attack signature or characteristic information related to the DoS attack with similar information detected at other routers 22b and 22c in the computer network system 10. DoS attack signatures that substantially match are grouped and implicitly form a path from the source of the DoS attack (*i.e.*, computer system 17) to the target (*i.e.*, computer system 16a).

This is to be contrasted with the directed tracing approach, where a general attack profile is extracted from every router's statistics to uncover the global path for the DoS attack packet.

As indicated at page 19, lines 13-20, the specific trajectory of the attack from the computer 17 of Zone U located in the computer network 14b (*i.e.*, Figure 4) to the computer system 16a of Zone X located in the computer network 14a is illustrated by the DoS attack path 100 (dashed line in Figure 7). The DoS attack path 100 commences at the attacking computer system 17 and extends through the routing system 20d, through the collector 20c, through the controller 24b, through the computer network 18, through the controller 24, through the collector 20, through the routing system 22, and to the targeted computer system 16a.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

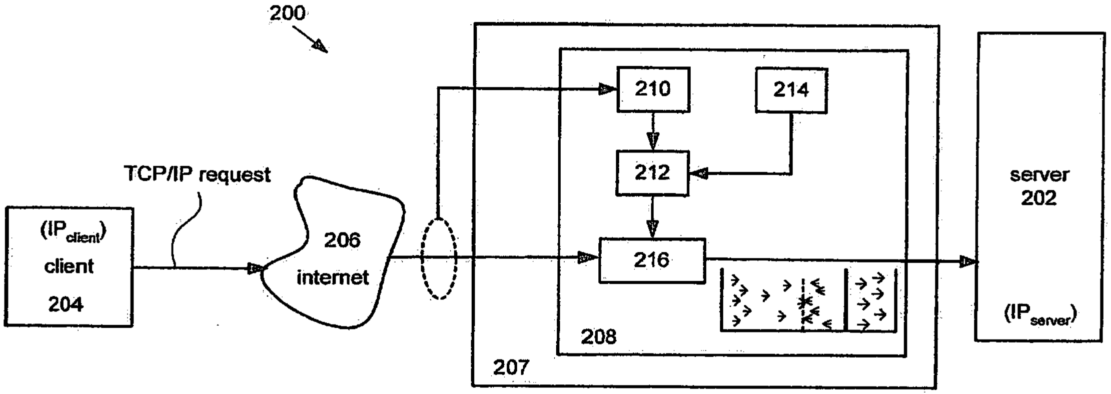
Claims 1-19, 21-23 and 26-33 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,789,203.

VII. ARGUMENT

A. Claims 1, 19 and 27 are Patentable Under 35 U.S.C. § 102(e) Over U.S. Patent No. 6,789,203 (Belissent)

The U.S. Patent to Belissent is primarily concerned with preventing a denial of service attack without notifying the attacker. The invention of Belissent is an IP throttler for defending against a denial of service attack and recording all connecting IP addresses by allowing its server to detect attackers as soon as the volume of connection requests coming from a particular IP address is higher than would otherwise be expected.

Fig. 2



As indicated at column 5, lines 36-50, and with reference to the above Figure 2 of Belissent, a firewall is included in or coupled to a server computer 202 which monitors all incoming connection requests. The firewall includes a throttler unit 208 that is used to identify and prevent any denial of service attacks. The throttler unit 208 includes a connection request monitor 210 arranged to monitor the number of connection requests received by a particular requesting client 204 based on the requesting client's IP address. A processor unit 212 is configured to count the number of connection requests for a particular requestor based on the associated IP address per unit of time.

Belissent fails to disclose the generation of one or more signals or alert message representing anomalies based on processed packet flow statistics which signal(s) is responded to by tracking or tracing attributes related to the anomalies to a source or origin of the attacks.

Contrary to the Examiner's assertion, "tracking" or "tracing" of the present invention is not equivalent to either "identifying" or "detecting" a denial service attack. Only the present invention describes and claims tracking one or more denial of service attacks over a computer network, as emphasized at numerous locations in the specification and claims. Such "tracking" or "tracing" is only done after detecting data packet flow anomalies or a DoS attack, which feature is found in independent claims 1, 19 and 27.

In summary, Belissent simply does not describe "tracing" or "tracking" back to the source or origin of an attack as only described and claimed in the present application.

The fee of $250.00 as applicable under the provisions of 37 C.F.R. § 41.20(b)(2) is enclosed. Please charge any additional fee or credit any overpayment in connection with this filing to our Deposit Account No. 02-3978.

Respectfully submitted,

Gerald R. Malan et al.

By:

David R. Syrowik
Registration No. 27,956
Attorney for Applicants

Date: 9-16-05

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351

Enclosure - Appendices

VIII. CLAIMS APPENDIX

1. A system for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising:

a collector adapted to receive a plurality of data packet flow statistics from a routing system of the computer network and to process the plurality of data packet flow statistics to detect one or more data packet flow anomalies and to generate a signal representing the one or more data packet flow anomalies; and

a controller coupled to the collector to receive the signal;

wherein the controller is constructed and arranged to respond to the signal by tracking attributes related to the one or more data packet flow anomalies to at least one source, and wherein the controller is constructed and arranged to block the one or more data packet flow anomalies.

2. The system of claim 1, wherein the collector includes a buffer coupled to the computer network and being adapted to process the plurality of data packet flow statistics to generate at least one record.

3. The system of claim 2, wherein the collector further includes a profiler coupled to the buffer and being adapted to receive and process the record to generate a predetermined threshold.

4. The system of claim 3, wherein the profiler includes means for aggregating the data packet flow statistics to obtain a traffic profile of network flows.

5. The system of claim 4, wherein the data packet flow statistics are aggregated based on at least one invariant feature of the network flows.

6. The system of claim 4, wherein data packet flow statistics are aggregated based on temporal, static network and dynamic routing parameters.

7. The system of claim 5, wherein the at least one invariant feature includes source and destination endpoints.

8. The system of claim 3, wherein the collector further includes a detector coupled to the buffer and to the profiler, the collector being adapted to receive and process the record and the predetermined threshold to detect if attributes associated with the record exceed the predetermined threshold representing the one or more data packet flow anomalies.

9. The system of claim 8, wherein the collector further includes a local controller coupled to the detector and to the profiler and being adapted to receive and respond to the one or more data packet flow anomalies by generating the signal representing the one or more data packet flow anomalies.

10. The system of claim 9, wherein the detector includes a database for storing the at least one record, predetermined threshold, the one or more data packet flow anomalies, and related information.

11. The system of claim 10, wherein the profiler includes a database for storing a plurality of data packet flow profiles and related information.

12. The system of claim 1, wherein the controller includes a filtering mechanism for blocking the one or more data packet flow anomalies.

13. The system of claim 12, wherein the filtering mechanism includes a plurality of filter list entries.

14. The system of claim 12, wherein the filtering mechanism includes a plurality of rate limiting entries.

15. The system of claim 1, wherein the controller includes a correlator coupled to the collector and being adapted to receive and normalize the plurality of signals representing the one or more data packet flow anomalies and to generate an anomaly table including the attributes related to the one or more data packet flow anomalies.

16. The system of claim 15, wherein the correlator includes a database for storing the anomaly table.

17. The system of claim 16, wherein the correlator further includes an adapter that is constructed and arranged to communicate the anomaly table to a computing device for further processing.

18. The system of claim 16, wherein the controller further includes:

a web server; and

access scripts that cooperate with the web server to enable a computing device to access the database defined on the controller to view the anomaly table.

19. A system comprising:

at least one routing system;

a plurality of computer systems coupled to the routing system;

means for detecting one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system based on a plurality of data packet flow statistics from the at least one routing system wherein the means for detecting includes a means for generating a plurality of signals representing one or more data packet flow anomalies; and

a means for tracking one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system wherein the means for tracking includes a means for receiving and responding to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies back to at least one source of the attack.

21. The system of claim 19, further including a means for blocking the one or more denial of service attacks communicated to the plurality of computer systems over the at least one routing system.

22. The system of claim 21, wherein the means for detecting includes a means for collecting ~~a~~ the plurality of data packet flow statistics from the at least one routing system.

23. The system of claim 22, wherein the means for detecting further includes a means for processing the plurality of data packet flow statistics to detect one or more data packet flow anomalies.

26. The system of claim 19, further including a means for communicating the one or more denial of service attacks to a computing device for further processing.

27. A method for detecting, tracking and blocking one or more denial of service attacks over a computer network, the system comprising the steps of:

collecting a plurality of data packet flow statistics from a routing system of the computer network;

processing the plurality of data packet flow statistics to detect one or more data packet flow anomalies;

generating a plurality of signals representing the one or more data packet flow anomalies; and

receiving and responding to the plurality of signals by tracking attributes related to the one or more data packet flow anomalies to at least one source.

28. The method of claim 27, further including the step of blocking the one or more data packet flow anomalies in close proximity to the at least one source.

29. The method of claim 28, wherein the step of collecting the plurality of data statistics includes:

buffering the plurality of data packet flow statistics;

processing the plurality of data packet flow statistics to generate at least one record; and

receiving and profiling the at least one record to generate a predetermined threshold.

30. The method of claim 29, wherein the step of collecting the plurality of data packet flow statistics further includes;

detecting if attributes related to the at least one record exceed the predetermined threshold representing the one or more data packet flow anomalies.

31. The method of claim 30, wherein the step of collecting the plurality of data packet flow statistics further includes: responding locally to the one or more data packet flow anomalies by generating the plurality of signals representing the one or more data packet flow anomalies.

32. The method of claim 27, wherein the step of receiving and responding to the plurality of signals includes:

correlating the plurality of signals representing the one or more data packet flow anomalies; and

generating an anomaly table including the attributes related to the one or more data packet flow anomalies.

33. The method of claim 32, wherein the step of receiving and responding to the plurality of signals further includes the step of communicating the anomaly table to a computing device for further processing.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.